On Hierarchical Threshold Access Structures

Kerem Kaşkaloğlu[1], Ferruh Özbudak[2]
[1]Department of Mathematics, Atilim University, Ankara
[2]Institute of Applied Mathematics, Middle East Technical University, Ankara
TURKEY

keremk@atilim.edu.tr, ozbudak@metu.edu.tr

ABSTRACT

One of the recent generalizations of (*t, n*) secret sharing for hierarchical threshold access structures is given by Tassa, where he answers the natural question of sharing a secret among a set of participants, say military officers, so that the secret can be constructed by a group of participants, some of whom are hierarchically superior to others. Both recent schemes proposed by Tassa for addressing this problem require some significant amount of theoretical background. We give a conceptually simpler alternative for the understanding of the realization of hierarchical threshold access structures and we consider perfectness of our scheme with the help of computer experiments. Our simple scheme employs a slightly different approach than previous works, as it involves a certain distribution of polynomials, where members of higher compartments are given a summation of evaluations of higher number of polynomials, resulting in a hierarchical effect. We further consider some alternative hierarchical access structures having potential to be applied in military. The access structures that we consider are realized herein with a simple employment of the well known building blocks such as Lagrange interpolation and access structure product and can be realized with an information rate at worst 1/m.

1.0 INTRODUCTION

The foundation of secret sharing is assumed to start with Shamir [1] and Blakley [2] who independently introduced *t-out-of-n*, or simply (t,n) secret sharing schemes (SSS) that allow a set of at least t participants to recover a secret while any t-1 or less participants fail in such an attempt. A secret sharing scheme is called *perfect* if a non-authorized participant set can learn no information about secret, while an authorized set recovers the secret. Simmons [3] introduced generalizations of (t,n) secret sharing, namely *hierarchical* and *compartmented* threshold secret sharing. In these multipartite approaches, the trust is not distributed uniformly among the set of participants. Letting U= $\bigcup_{i=1}^{m} C_i$ be the set of participants which is partitioned into m disjoint subsets of compartments C_i, $1 \le i \le m$, a *multipartite access structure* $\Gamma \in 2^U$ is one that does not distinguish between members of the same compartment. It is reasonable to assume that access structures are monotone, i.e., if $A \in \Gamma$ and $A \subset B \subseteq U$, then $B \in \Gamma$. A well known measure of efficiency for SSS's is the notion of *information rate*, which is concerned with the size of the private data (shares of participants) used for sharing a secret of certain size. A secret sharing scheme is called *ideal* if the domain of shares of each user equals to the domain of secrets, yielding to an information rate 1. An access structure Γ is ideal if for some finite domain of shares, there exists an ideal secret sharing scheme realizing it.

Hierarchical access structures that admit an ideal secret sharing scheme are characterized within a unified framework in [9]. There are three main types of ``hierarchy-involved'' access structures in literature. Those are, in chronological order, Shamir's weighted threshold access structures [1], Simmons' hierarchical access structures [3] which answer the question of solving a secret by either two vice presidents or three bank tellers (where a vice president can always replace a bank teller) and Tassa's hierarchical threshold access structures [4] raising an answer to the problem of sharing a secret among three employees, say again composed of vice presidents and bank tellers, at least two of which is a vice president. The main

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE
On Hierarchical Threshold Access Structures

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Department of Mathematics, Atilim University, Ankara

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT

One of the recent generalizations of (t, n) secret sharing for hierarchical threshold access structures is given by Tassa, where he answers the natural question of sharing a secret among a set of participants, say military officers, so that the secret can be constructed by a group of participants, some of whom are hierarchically superior to others. Both recent schemes proposed by Tassa for addressing this problem require some significant amount of theoretical background. We give a conceptually simpler alternative for the understanding of the realization of hierarchical threshold access structures and we consider perfectness of our scheme with the help of computer experiments. Our simple scheme employs a slightly different approach than previous works, as it involves a certain distribution of polynomials, where members of higher compartments are given a summation of evaluations of higher number of polynomials, resulting in a hierarchical effect. We further consider some alternative hierarchical access structures having potential to be applied in military. The access structures that we consider are realized herein with a simple employment of the well known building blocks such as Lagrange interpolation and access structure product and can be realized with an information rate at worst 1/m.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**12**	

difference among the last two structures is that the former is a disjunction of different compartments representing distinct hierarchy levels, whereas the latter is a conjunction of such compartments. Both definitions consider the case where some of the participants are hierarchically superior to others. The definition of the access structure given in [4] is as follows. Letting U= $\bigcup_{i=1}^{m} C_i$ be the set of participants with disjoint compartments C_i ,$1 \le i \le m$,

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |V \cap (\bigcup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \ \ \forall i \in \{1, \ldots, m\}\} \qquad (1)$$

Under the same assumptions of above definition, the former hierarchical access structure that is studied by Simmons is as follows.

$$\Gamma = \{\mathcal{V} \subset \mathcal{U}, \exists i \in \{1, \ldots, m\} : |\mathcal{V} \cap (\bigcup_{j=1}^{i} \mathcal{U}_j)| \geq k_i\} \qquad (2)$$

Previous Work. Besides proposing such hierarchical threshold access structures, Tassa gave an ideal SSS for their realizing in [4]. To reconstruct the secret, he used Birkhoff interpolation using some derivative values of a polynomial. This approach took attention and found place in recent applications, an example of which is employment in ad hoc networks [10]. Birkhoff interpolation is performed in a setting that the given values of the unknown polynomial, *P(x)*, also include derivative values. Specifically, participants from level C_i, $1 \le i \le m$ receive the value of the t_{i-1}^{th} derivative (t_0=0) of *P* at the point that identifies them. Allowing participants from higher levels have shares such as derivatives of *P* of lower orders, naturally let shares of such participants carry more information on the coefficients of *P* than shares of participants from lower levels. Later on, Tassa and Dyn [5] proposed another scheme for threshold access structures, which demands calculation of t_m restrictions of a bivariate polynomial to a line each of which is followed by a univariate Lagrange interpolation. We would like to note that the aforementioned works [4],[5] and the modified scheme we give herein are ideal and linear in the sense of Brickell's [7].

The reconstruction phase of a linear SSS in essence corresponds to solving some linear system. For a random allocation of participant identities, the hierarchical schemes in [4] and [5] and ours are perfect in a probabilistic manner. That is, when the underlying field *F* is large enough, the probability that an authorized set not being able to reconstruct the secret together with the probability that a non-authorized set reconstructs the secret is negligible.

Our Strategy. The only two schemes for hierarchical threshold access structures [4] and [5] apply Birkhoff interpolation and subsequent univariate Lagrange interpolation respectively. In the very essence, both methods correspond to solving a linear system of equations at the end. Instead of applying any kind of interpolation techniques, we present a scheme that directly leads us again to a linear system of equations. Letting m to represent the number of compartments, we give summation of evaluations of m polynomials at some public points to the highest compartment in the hierarchy, summation of evaluations of m-1 polynomials in the second highest level, and continuing this manner, evaluation of only 1 polynomial to the lowest compartment of the hierarchy. They are combined in a manner that participants from the highest levels can always replace the lower-leveled ones whereas the converse does not hold.

Organization of the Paper. After introducing some preliminaries in section 2, we give our ideal scheme for hierarchical threshold access structures in section 3, where an example together with a table of experimental results is included. In section 4, we consider how Lagrange interpolation and access structure product can be employed to obtain a variety of alternative hierarchical access structures. We conclude with some remarks on section 5.

2.0 PRELIMINARIES

ILSSS. In an ideal linear secret sharing scheme(ILSSS) over a finite field *F*, the domain of secrets is equal to *F* (so that the scheme is ideal) and the scheme is specified by n+1 vectors in F^d where d is an integer. Such vectors are as follows. The dealer uses a vector $\mathbf{u_i}$ for each participant u_i belonging to U, $1 \le i \le n$, and a vector **t** which is kept private. To share a secret $S \in F$, the dealer chooses a random vector $\mathbf{w} \in F^d$ such that the inner product **w.t**=S and distribute each share $\mathbf{w}.\mathbf{u_i}$ to participant u_i.

Shamir's SSS. The basic linear scheme proposed by Shamir [1], makes use of Lagrange's polynomial interpolation. The scheme works as follows: Let q be a large prime and $S \in F_q$ be the secret to be shared. The dealer chooses a random univariate polynomial $f(x)=S+\sum_{i=1}^{t-1} a_i x^i \in F_q$ of degree t-1 where the constant term is the secret. In order to distribute S among n participants given by $u_1,...,u_n$ assign to the j-th participant the share $f(u_j)=S+\sum_{i=1}^{t-1} a_i u_j^i, 1 \le j \le n$.

While the reconstruction of the secret can be described by a formula resulting from Lagrange's polynomial interpolation, a linear algebra point of view heads us towards the following linear system that the authorized subset of participants $\{u_{i_1},...,u_{i_t}\}$, $1 \le i_1 < ... < i_t \le n$ must solve.

$$\begin{pmatrix} 1 & u_{i_1} & \dots & u_{i_1}^{t-1} \\ \vdots & & & \\ 1 & u_{i_t} & \dots & u_{i_t}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} f(u_{i_1}) \\ \vdots \\ f(u_{i_t}) \end{pmatrix}$$

As pointed out by Shamir himself in [1], a hierarchical variant can be introduced simply by assigning a higher number of shares to higher level participants. However such a solution is far away from being ideal. While Shamir's SSS, having a Vandermonde matrix on its basis, enjoys the property of reconstructibility of the secret with probability exactly 1, by an authorized subset, as mentioned earlier, the schemes given in [4],[5] and the scheme we propose in the next section claims this property with a probability merely close to 1 depending on the field size and some constants.

Linear SSS's (LSSS) are widely studied under the notion of monotone span programs (MSP). Formally, a MSP is a 5-tuple $\mathbf{M}=(F,M,U,\varphi,\mathbf{t})$, where *F* is a field, M is a matrix of dimensions dxe over *F*, $U=\{u_1,...,u_n\}$ is a finite set, $\varphi: \{1,...,d\} \rightarrow U$ is a surjective function assigning each row to a participant in U, and $\mathbf{t} \in F^e$ is the so-called target vector. Participants are said to own or privately hold one or more certain row(s) of M. The MSP **M** is said to realize (compute) the monotone access structure Γ in case that **t** is spanned by the rows of the matrix M_V if and only if $V \in \Gamma$, where M_V is the matrix whose rows are formed by participants of the set $V \in U$. The size of **M** is d, the number of rows of M. Indeed, the size of the MSP is the total number of shares that are distributed to all participants in U.

Now giving share s_i to participant $\varphi(i)$, we can identify an LSSS with its underlying MSP. It is known, due to [6], that every monotone access structure admits a secret sharing scheme, but it is often the case that shares must be larger than the secret.

If Γ is a monotone access structure realizing U, its dual $\Gamma^* = \{V : V^c \notin \Gamma\}$ is also monotone and if **M** is an MSP that realizes Γ, then its dual $\mathbf{M}^*$ of the same size as **M** exits and realizes the dual access structure Γ^*. $\mathbf{M}^*$ can be efficiently constructed as described in [8]. An access structure is ideal if and only if its dual is. Given two monotone access structures Γ_1 and Γ_2 defined on sets of participants U_1 and U_2

respectively, one can define the product Γ_1 x Γ_2 as the monotone access structure defined on $U_1 \cup U_2$ such that for any $V \subseteq U_1 \cup U_2$ it holds that $V \in \Gamma_1$ x $\Gamma_2 \Leftrightarrow (V \cap U_1 \in \Gamma_1$ and $V \cap U_2 \in \Gamma_2)$

The following is a well-known realization of the product Γ_1 x Γ_2.

Lemma 1. *If MSPs $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ with matrices $M_1=(c_1\ M_1')$ and $M_2=(c_2\ M_2')$ (where c_1 and c_2 are the first columns of the matrices) and target vectors $\boldsymbol{1}=(1,0,...,0)$ realize the access structures Γ_1 and Γ_2 respectively, then the matrix*

$$\begin{pmatrix} c_1 & \mathbf{0} & M_1' & 0 \\ 0 & c_2 & 0 & M_2' \end{pmatrix}$$

realizes Γ_1 x Γ_2 with target vector (1,1,0,...,0).

The reason that the first columns of the matrices $M_1$and M_2 has been taken out is to simply be able to use the target vector (1,1,0,...,0). One can directly employ matrices $M_1$and M_2 without separating their first columns c_1 and c_2 as long as a target vector such as (1,0,...,0,1,0,...,0) is used. Note that the definition of product of two access structures, Γ_1 x Γ_2, and lemma 1 can naturally be extended to Γ_1 x Γ_2 x ... x Γ_k in a straightforward manner.

Lemma 2. *Given MSPs $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ realizing access structures Γ_1 and Γ_2 defined on sets U_1 and U_2 respectively,*

i) if $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ are ideal and U_1 and U_2 are disjoint sets, then $\boldsymbol{M}_1$ x $\boldsymbol{M}_2$ is also ideal.
ii) if $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ are perfect, so is $\boldsymbol{M}_1$ x $\boldsymbol{M}_2$.

Proof. If $\mathbf{M}_1$ and $\mathbf{M}_2$ are ideal, participants from Γ_1 and Γ_2 own one and only one row apiece in the corresponding matrices M_1 and M_2, respectively. Let the reconstruction matrix of Γ_1 x Γ_2 be M_{1x2}. Then participants of Γ_1 x Γ_2 will obviously own one row in M_{1x2} as well, since no participant who is both in U_1 and U_2 exists. Similarly if $\mathbf{M}_1$ and $\mathbf{M}_2$ are perfect, determinants $|M_1|$ and $|M_2|$ will be nonzero for every possible sets of authorized participants in Γ_1 and Γ_2 respectively, yielding to a nonzero determinant $|M_{1x2}|=|M_1|.|M_2|$.

3.0 THE MODIFIED SCHEME

To extract the allowance of maximum number of participants from each compartment while recalling (1), define $t_i=k_i-k_{i-1}, 1 \le i \le m$ (assume $k_0=0$). Observe that $\sum_{i=1}^{m} t_i = k_m$. Now the following describes a SSS to realize (1), namely hierarchical threshold access structures.

Secret sharing scheme 1.
1. The dealer generates m random polynomials $P_i(x) = \sum_{j=1}^{t_i} a_{ij}x^j,\ 1 \le i \le m$ so that $deg(P_i(x)) = t_i$ and the secret $S = \sum_{i=1}^{m} a_{i1}$.
2. Each participant c_{ij} from compartment $\mathcal{C}_i$ will be identified by a unique public point (x_{ij}, y_{ij}), $x_{ij} \neq 0, y_{ij} \neq 0$, where no two participant is given the same x_{ij} or y_{ij} value. The private share of the participant c_{ij} will be $Q_i(x_{ij}, y_{ij}) = \sum_{\ell=i}^{m} y_{ij}^{\ell} P_\ell(x_{ij})$.

In step 2, the purpose of multiplying the polynomials $P_\ell(x_{ii})$ with y_{ii}^{ℓ} in the bivariate polynomial Q_i is simply to prevent the occurrence of identical columns in the reconstruction matrix so that the determinant

does not turn out to be zero (we will consider the importance of determinant in the proof of theorem 1). In the reconstruction phase, we let the rows of participants from higher compartments involve more variables by such a distribution of polynomials. In more detail, the row given to members of compartment C_1 involves a summation of all polynomials $P_i(x)$, hence involving $\sum_{i=1}^{m} t_i$ variables. Similarly, the row given to members of compartment C_2 involves $\sum_{i=2}^{m} t_i$ variables, whereas the polynomial corresponding to the lowest level compartment C_m involves only t_m variables. This decreasing number of variables constitutes the main idea that produces a hierarchical effect. Obviously, the scheme is ideal as the shares of participants are taken from the domain of secrets *F*. Observe that the problem of recovering the secret in the above scheme is equivalent to solving the whole system, that is, there is no easy shortcut of obtaining only the polynomial coefficients a_{i1}, i=1,...,m that sum up to the secret S.

Theorem 1. *An authorized set $V \in \Gamma$ may recover the secret S with a probability bounded by $1-2k_m dq^{-1}$ where m is the number of compartments, k_m is the order of the reconstruction matrix, q is the size of the field and d is the degree of the variables in det(M).*

Proof. We apply techniques in analogy with the ones used in the proofs of [5]. Notice that the reconstruction matrix M is k_m x k_m where $k_m=t_1+...+t_m$. Consider the equation M.A=Q where M is the reconstruction matrix formed by an authorized set of participants, $A=(a_{11} \dots a_{1t_1}\ a_{21} \dots a_{2t_2} \dots\ a_{m1} \dots a_{mt_m})^t$ is the vector of unknowns involving the secret and Q is the vector formed by private shares of participants. Employing basic linear algebra, we know that such an equation has a unique solution if and only if $det(M) \neq 0$. That is, the probability that an authorized set can reconstruct the secret equals to the probability of $det(M) \neq 0$ where M is their corresponding reconstruction matrix. Since the values x_{ij} and y_{ij} in the reconstruction matrix are random, the determinant is a random value over *F*. So the idea is that, the larger the underlying field *F* gets, the smaller the probability that the reconstruction matrix has determinant zero. And if the determinant is nonzero, then it is obvious that one can find its inverse and solve the unknown vector together with the secret embedded therein. Observe that there are two distinct variables in each of the k_m rows. So considering the expansion of M, we see that *det(M)* is a nonzero polynomial of $2k_m$ variables over the finite field *F*, where the highest degree of the variables in *det(M)* can be expressed as $d = \max(t_i)$, $1 \leq i \leq m$. Now applying lemma 2.2 of [4], we see that the number of zeros of *det(M)* in F^{2k_m} is bounded by $2k_m dq^{2k_m-1}$. Indeed, these are all the choices that make det(M)=0 among all possible q^{2k_m} selections of the $2k_m$ variables. So the probability that det(M)=0 is bounded by $2k_m dq^{2k_m-1}\ q^{-2k_m} = 2k_m dq^{-1}$.

Observe that the distribution of entries of a reconstruction matrix M is similar to that of an upper triangular matrix. The reconstruction matrix employed in the proof of theorem 4 in [4] also has a triangular structure which seems to be rather in lower triangular-like form. Indeed this triangularity is the main specialty that gives a scheme characteristics of a hierarchical threshold secret sharing. For a random allocation of participant identities, with a high probability depending on the size of the field *F*, scheme 1 perfectly realizes (1) as in the case of the corresponding scheme given in [4]. However, perfectness with probability 1 under a monotone allocation of participant identities provided in [4] is not satisfied in scheme 1.

Example 1. Let m=3 be the number of compartments where, $k_1=2$, $k_2=5$, $k_3=8$ yielding polynomials $P_1(x),P_2(x),P_3(x)$ of degrees respectively $t_1=2$, $t_2=3$, $t_3=3$. Finally, let $s_1=2$, $s_2=4$,$s_3=2$ be the number of participants from compartments C_1, C_2, C_3 respectively. Then M is of the form;

$$M = \begin{pmatrix} x_{11}y_{11} & x_{11}^2y_{11} & x_{11}y_{11}^2 & x_{11}^2y_{11}^2 & x_{11}^3y_{11}^2 & x_{11}y_{11}^3 & x_{11}^2y_{11}^3 & x_{11}^3y_{11}^3 \\ x_{12}y_{12} & x_{12}^2y_{12} & x_{12}y_{12}^2 & x_{12}^2y_{12}^2 & x_{12}^3y_{12}^2 & x_{12}y_{12}^3 & x_{12}^2y_{12}^3 & x_{12}^3y_{12}^3 \\ 0 & 0 & x_{21}y_{21}^2 & x_{21}^2y_{21}^2 & x_{21}^3y_{21}^2 & x_{21}y_{21}^3 & x_{21}^2y_{21}^3 & x_{21}^3y_{21}^3 \\ 0 & 0 & x_{22}y_{22}^2 & x_{22}^2y_{22}^2 & x_{22}^3y_{22}^2 & x_{22}y_{22}^3 & x_{22}^2y_{22}^3 & x_{22}^3y_{22}^3 \\ 0 & 0 & x_{23}y_{23}^2 & x_{23}^2y_{23}^2 & x_{23}^3y_{23}^2 & x_{23}y_{23}^3 & x_{23}^2y_{23}^3 & x_{23}^3y_{23}^3 \\ 0 & 0 & x_{24}y_{24}^2 & x_{24}^2y_{24}^2 & x_{24}^3y_{24}^2 & x_{24}y_{24}^3 & x_{24}^2y_{24}^3 & x_{24}^3y_{24}^3 \\ 0 & 0 & 0 & 0 & 0 & x_{31}y_{31}^3 & x_{31}^2y_{31}^3 & x_{31}^3y_{31}^3 \\ 0 & 0 & 0 & 0 & 0 & x_{32}y_{32}^3 & x_{32}^2y_{32}^3 & x_{32}^3y_{32}^3 \end{pmatrix}_{8\times 8}$$

We leave the fulfillment of polynomials and arbitrary parameters of the scheme to the reader. We provide an extensive table of probabilistic results regarding secret sharing scheme 1 with assistance of a computer algebra system [11] where results in each of the entries are obtained by 10^5 experiments with distinct random allocation of x_{ij} and y_{ij} values.

Table 1: Success Rates of Reconstructibility of the Secret

$k_i, t_i,\ 1 \le i \le m$	$s_i,\ 1 \le i \le m$	q=101	q=100003
$k_1 = 2, k_2 = 5, k_3 = 9$ $(t_1 = 2, t_2 = 3, t_3 = 4)$	$s_1 = 4, s_2 = 4, s_3 = 1$	impl: 0.9876	impl: 0.9999
	$s_1 = 2, s_2 = 3, s_3 = 4$	impl: 0.9039	impl: 0.9998
	$s_1 = 9, s_2 = 0, s_3 = 0$	impl: 0.9867 theo: 0.2872	impl: 0.9999 theo: 0.9993
$k_1 = 1, k_2 = 4, k_3 = 10, k_4 = 23$ $(t_1 = 1, t_2 = 3, t_3 = 6, t_4 = 13)$	$s_1 = 4, s_2 = 2, s_3 = 8, s_4 = 9$	impl: 0.8668	impl: 0.9995
	$s_1 = 1, s_2 = 5, s_3 = 12, s_4 = 5$	impl: 0.8441	impl: 0.9992
	$s_1 = 23, s_2 = 0, s_3 = 0, s_4 = 0$	impl: 0.9650 theo:0.0	impl: 0.9999 theo: 0.9940

Observe that all the experimental results (impl.) in table 1 are greater than theretical bounds (theo.) obtained by the formula according to theorem 1. It can also be seen that, for artificially small values of q, the given bound is loose and sometimes it does not provide any information. Even in these cases, our modified scheme yields quite acceptable results for small m values. As $q \to \infty$, the aforementioned probabilities get closer to 1. Indeed, as k_i values increase, higher q values will be needed to keep the probability of the success rate constant. The table, considering some extreme cases, also visualizes the fact that the distribution of s_i values $1 \le i \le m$ affects the experimental probabilistic results.

4.0 (C,M) HIERARCHICAL ACCESS STRUCTURES

4.1 Motivation and The Scheme

Let us first recall hierarchical threshold access structures introduced in [4]. Let $U = \bigcup_{i=1}^{m} U_i$ be the set of participants with m disjoint levels, i.e.,$i\ U_i \cap U_j = \varnothing$, $1 \le i < j \le m$ and let $k_i{}_{i=1}^{m}$ be a sequence of integers with $0 < k_1 < \ldots < k_m$. Then the corresponding hierarchical threshold access structure is

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \ge k_i \quad \forall i \in \{1, \ldots, m\} \right\} \quad (1)$$

Under the same assumptions of the above definition, the former hierarchical access structure that is studied by Simmons is as follows.

$$\Gamma = \left\{\mathcal{V} \subset \mathcal{U}, \exists i \in \{1,\ldots,m\} : |\mathcal{V} \cap (\cup_{j=1}^{i}\mathcal{U}_j)| \geq k_i\right\} \quad (2)$$

Observe that the only difference in (2) is the replacement of the universal quantifier $\forall$ with the existential quantifier $\exists$. If we identify the requirement $|\mathcal{V} \cap (\cup_{i=1}^{i}\mathcal{U}_j)| \geq k_i$ as the threshold condition to be satisfied by levels U_j, $j \leq i$ yielding m conditions, then the distinction among (1) and (2) is that while Simmons' version exploits a disjunction of threshold conditions, Tassa's definition involves a conjunction of such conditions. Letting the c be the threshold number for conditions to be satisfied among m, the definitions above describe access structures that either demand the presence of exactly one of such conditions (c=1) or all of them simultaneously (c=m). That is, neither of the definitions above has flexibility to contain the intermediary access structures corresponding to values of 1<c<m . With this motivation, we consider the following generalization of the access structures (1) and (2).

Definition 1. *Let $\mathcal{U} = \bigcup_{i=1}^{m}\mathcal{U}_i$ be the set of participants with m disjoint levels, i.e., $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, for $i \neq j$. Let $\{k_i\}_{i=1}^{m}$ be a sequence of integers with $0 < k_1 < \ldots < k_m$. Then the corresponding (c,m) hierarchical access structure is*

$$\Gamma = \left\{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i}\mathcal{U}_j)| \geq k_i \text{ for at least } c \text{ indices } i \in \{1,\ldots,m\}\right\} \quad (3)$$

In Tassa's seminal work [4], the generalization (3) is indeed mentioned and a question asking whether it is an ideal access structure or not, is raised. To the best of our knowledge, no known SSS applies for the case of (c,m) hierarchical access structures for 1<c<m. Though we do not attempt to solve the open problem stated by Tassa, we give a non-ideal scheme realizing (3) and discuss the difficulty of establishing an ideal scheme for the realization of [4] in the section 4.2. It follows from the definition that a (c,m) hierarchical access structure is also a (c',m) hierarchical access structure for c'<c. Let us give a toy illustration of (3).

Example 2. Consider a scenario where a secret is to be shared among participants from levels U_1 , U_2 and U_3 which are formed by admirals, brigadiers and colonels respectively. Let us represent each participant of a certain level by the initial of the identifier of the level. That is, for instance, the phrase *aab* stands for a set formed by two admirals and one brigadier. Now m=3 and let k_1=1, k_2=2 and k_3=3 for the sake of simplicity. The minimal authorized sets in the (c,m) hierarchical access structures, c={1,2,3}, according to definition 1 is as follows.

	minimal authorized sets in (c,3) hierarchical access structure
$c = 1$	$\{a, bb, ccc, bcc\}$
$c = 2$	$\{aa, ab, acc, bbb, bbc\}$
$c = 3$	$\{aaa, aab, abb, abc\}$

Here, the term *minimal authorized set*, sometimes being called *minterm*, refers to a qualified set such that no participant within the set is redundant for the reconstruction of the secret. It is exemplified that all minimal subsets of (1) are of the same size while this is not true for (2) and (3). The k_i values suggest that basically all the sets 1 admiral, 2 brigadiers and 3 colonels are of equal trust. Regarding involvement of each of the sets *a*, *bb* and *ccc* (while keeping in mind the fact that the lower level participants can always be replaced by upper level ones) as a condition to be imposed on an access structure, it is perfectly natural in real life to require any two of these conditions to be present as well as demanding either one of the conditions or all three of them simultaneously.

One can mimic the realization of the (2,3) hierarchical access structure of example 2 with a naive employment of Shamir's weighted threshold secret sharing [1], by say assigning 3 shares to each admiral, 2 shares to each brigadier and 1 share to each colonel and establishing a (5,n) SSS among the n participants via the well-known Lagrange interpolation. In this case, all the required the minimal

authorized sets {*aa*,*ab*,*acc*,*bbb*,*bbc*} are eligible to reconstruct the secret. However, the access structure of such a scheme would embody a set of participants such as *ccccc* which is not the case for (2,3) hierarchical access structure arousing from definition 1. Nevertheless, we can tailor a scheme for this particular case again via the well-known tools such as Lagrange interpolation and access structure product, but this time, with a different distribution of shares. The scheme can be described as follows.

Scheme 2. To realize (3), assign one secret for each level and apply a scheme of Shamir's in a setting that each participant belonging to that level and the participants in the upper levels are given shares. That is, the dealer first applies a (c,m) Shamir's scheme on the secret to obtain m private partial shares, say s_1, …,s_m, so that any c of these values are sufficient to find the secret. Then he applies a separate Shamir's scheme on each s_i, $1 \leq i \leq m$, so that in each instance of such schemes, the shares are this time distributed to not only the members of the compartment U_i but also to the members of all compartments U_i ,…, U_{i-1} accomplishing the desired property that members of the upper level compartments can always replace participants of the lower ones. Here, each Shamir's scheme on the partial secret s_i will be arranged in a setting that s_i can be reconstructed only with the presence of any k_i-k_{i-1} shares (assuming k_0=0 for s_1). This allows that the partial share s_i can be computed if and only if k_i members from $\bigcup_{j=1}^{i} U_j$ are present. Hence for a set of participants, reconstruction of each s_i ensures one threshold condition in Γ of definition 1. Since we require any c of such threshold conditions among m, the purpose of applying first a (c,m) scheme on the secret follows.

4.2 Efficiency Issues, Perfectness and Discussions

In scheme 1, each participant from U_1 is given m shares; each participant from U_2 is given m-1 shares and so on. Eventually, a participant from the lowest level U_m is given only 1 share. In the order of operations performed for the reconstruction of the secret, there are m Lagrange interpolations each of which is to recover one of the partial secrets s_1,...,s_m, and there is one final occurrence of a (c,m) Shamir's scheme summing up to m+1 instances of Lagrange interpolations. Again, all these schemes can be combined by lemma 1. Since Lagrange interpolations are used as basic building blocks, the above scheme is perfect by lemma 2 and hence enjoys the property of reconstructability of the secret by an authorized set with probability 1.

An observation on the difficulty of establishing an ideal and efficient LSSS for the realization of [4] is as follows. In [9], it is proven that a multipartite access structure involving a hierarchy among participants is ideal if and only if the access structure admits a vector space secret sharing scheme. So if there exists an ideal and efficient scheme realizing (3), it must be in the form of a vector space scheme, that is an ideal linear scheme constructed according to the method proposed by Brickell. In such a scheme, we are allowed to assign one and only one public vector to each participant including the target vector of the dealer, so that the shares are computed by dot products of these vectors with a random (secret) vector. Within such a setting, the purpose is to design a scheme which both allows higher-leveled participants to replace their inferiors and assures the satisfaction of any c of the m conditions defined on levels. Such a design may not be easy especially when one considers the varying size of minimal authorized subsets, which makes things a little more complicated. We would like to remind the reader that finding an efficient, ideal and linear solution for the disjunctive case of Simmons has remained a long standing open problem and its realization became possible in [4], only when some duality techniques were employed to the efficient and perfect vector space construction of its conjunctive counterpart, which has fixed length minimal authorized subsets. However, this approach does not seem to apply to (3), as the dual of a (c,m) hierarchical access structure of the form (3) is a (m+1-c,m) hierarchical access structure, again having variable-length minimal authorized subsets for 1<c<m. Indeed, regarding compartmented and hierarchical (c,m) access structures, our intuition is that the schemes that we realize herein have already attained best possible information rates. However, this statement is no further realistic than a conjecture without a

proof. In [8], it is also shown that a hierarchical access structure admitting a scheme in which the length of every share is less than 3/2 times the length of the secret, is ideal, that is, it admits an ideal scheme as well. However, this condition is not satisfied by the scheme we provide. So we are unable to apply the mentioned result of [8] for the (c,m) hierarchical case.

A final remark on efficiency is that, in scheme 1, the number shares of a user is at most m, yielding to an information rate such as 1/m. However, we would like to note that, information rate is not he only notion of efficiency. Indeed, another similar complexity measure of secret sharing schemes is their share size, that is, the total length of all shares distributed by the dealer. Scheme 1 performs slightly better in the latter case than it does in the case of information rate. The reason is that, as there are typically more participants in the lower levels compared to that of higher ones, the average number of shares per user is usually lower than a worst case of (m+1)/2. The scheme we provide is obviously not be the best choice for the cases c=1 or c=m. However, to the best of our knowledge, it is the only scheme that realizes the intermediary access structures in between two former definitions involving a hierarchy, it is perfect and is efficient enough for scenarios with small parameters.

4.3 Fixing First k Levels

Observe that for the case c=2 of example 2, it is possible for a group of brigadiers and colonels to reconstruct the secret without the presence of any admiral. However, the dealer may desire the existence of at least one admiral in an authorized set, that is, while the members of the set {*aa,ab,acc*} remains authorized, *bbb* and *bbc* will be identified as non-authorized. To restate this in a more general sense, the top k compartments may be distinguished by the necessity of satisfaction of all the conditions defined upon them, whereas this is not the case for the remaining lower compartments. That is, one may fix the first k compartments and obtain the following generalization under the same setting of definition 1.

$$\Gamma' = \left\{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \ \ \forall i \in \{1,\ldots,k\} \text{ and for at least c indices } i \in \{k+1,\ldots,m\}\right\}$$

Here, k is the threshold value assuring that the conjunction of k conditions on the first k levels hold in an authorized set. Among the remaining m-k conditions left out, any c of them are considered to be enough. Γ' trivially becomes equivalent to Γ of definition 1 when k=0. A realization of Γ' is as follows.

Scheme 3. We combine Tassa's conjunctive scheme involving Birkhoff interpolation and scheme 2 in a way handling Γ'.The dealer first applies Tassa's conjunctive scheme to participants of first k levels U_i, $1 \leq i \leq k$. So far, members of levels $U_1,\ldots,U_k$ are given one share apiece. On the other hand, the dealer applies scheme 2 to members of the remaining levels $U_{k+1},\ldots,U_m$, so that a participant from level U_{k+1} is given m-k shares, a participant from level U_{k+2} is given m-k-1 shares and finally, each participant from level U_m is given only 1 share. For now, we have only partitioned the levels to two sets with indexes 1,…,k and k+1,…,m applying Tassa's conjunctive scheme and scheme 2 to each set respectively. The only missing part for the realization of Γ' is the allowance of members of $U_1,\ldots,U_k$ to substitute lover-leveled participants belonging to $U_{k+1},\ldots,U_m$. To allow this, we give a set of m-k additional shares to each member of levels $U_1,\ldots,U_k$. Such m-k shares are identical to the set of shares given to members of U_{k+1}, so that members of $U_1,\ldots,U_k$ can always replace members of $U_{k+1},\ldots,U_m$, which completes the scheme. The highest number of shares distributed belongs to members of levels $U_1,\ldots,U_k$, where each participant is given m-k+1 shares.

Tassa's conjunctive scheme [4] is proven to be perfect for a sufficiently large field via a monotone allocation of participant identities. So, with a perfect employment of Tassa's scheme and a series Shamir's schemes in the basis of scheme 2, perfectness follows from lemma 2. As an underlying scheme for first k levels, one can of course choose any other scheme realizing (1), say the one given in [5], instead of the one employing Birkhoff interpolation [4]. But if the chosen scheme is not perfect with certainity, scheme 2 will not reach perfectness with certainity either. Except that, the selection will not affect scheme 2.

It is described in [4] that the realization of the disjunctive access structure (2) can be achieved with the help of the conjunctive scheme realizing (1), and some duality techniques. On the other hand, scheme 2 is designed for the cases $1<c<m$ as it combines Tassa's conjunctive scheme for (1) and scheme 1. A particular case is as follows. When $c=1$ in Γ', one may alternatively combine both Tassa's conjunctive and disjunctive schemes and apply to compartments $U_1,\ldots,U_k$ and $U_{k+1},\ldots,U_m$ respectively to obtain a better information rate such as 1/2.

5.0 CONCLUSION

Our contribution. In the first part of this study, we consider an ideal and linear secret sharing scheme for the understanding of hierarchical threshold access structures and give some experimental analysis on the reconstructibility of the secret. In the second part of this work, we consider a generalization of the hierarchical access structure of Simmons' and the hierarchical threshold access structure of Tassa's. For this case, the linear scheme that we consider is not ideal but has a high information rate so that number of shares of a user is at most m and m/2 on average.

Future work. One may attempt to prove or hopefully disprove the conjecture that we discussed in section 4.2, regarding the nonexistence of an ideal, linear and efficient scheme for (3), perhaps with the involvement of the techniques similar to the ones in [9], which is out of the scope of this work. A constructive attempt for (3) might be designing a scheme with a better information rate, if there is any.

Acknowledgments. The authors would like to thank Ali Aydın Selçuk for useful discussions.

The authors were partially supported by TÜBİTAK under Grant No. TBAG-107T826.

REFERENCES

[1] A. Shamir, How to Share a Secret, *Comm. ACM*, vol. 22, no. 11, 1979, pp. 612-613.

[2] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, 1979, American Federation of Information Processing Societies Proceedings 48. 1979, pp. 313-317.

[3] G.J. Simmons, How to (really) share a secret, *Advances in Cryptology - CRYPTO 88*, LNCS 403, 1990, pp. 390-448.

[4] T.Tassa, Hierarchical Threshold Secret Sharing, *Cryptology*. 20, 237-264, 2007. An earlier version appeared in the proceedings of the First Theory of Cryptography Conference 2004, February, (MIT-Cambridge), 2004, pp. 473-490.

[5] T.Tassa, Multipartite Secret Sharing by Bivariate Interpolation, *J, Cryptology*. 22, 2009, 227-258.

[6] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In Proc. of the IEEE *Global Telecom. Conf., Globecom 87*, pages 99–102, 1987. Journal version: Multiple Assignment Scheme for Sharing Secret. *J. of Cryptology*, 6(1):15-20, 1993.

[7] E.F. Brickell, Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9, 1989, pp. 105-113.

[8] S.Fehr, Efficient construction of the dual span program. *Manuscript*, May 1999.

[9] Oriol Farras and Carles Padro, Ideal Hierarchical Secret Sharing Schemes, *Cryptology ePrint Archive*: Report 2009, 141.

[10] E. Ballico, G. Boato, C. Fontanari, and F. Granelli, Hierarchical Secret Sharing in Ad Hoc Networks through Birkhoff Interpolation, *K. Elleithy et al. (eds.), Advances in Computer, Information, and Systems Sciences, and Engineering*, 2006, pp. 157-164.

[11] Bosma W., Cannon J.: *The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry* (version 2.11-14). University of Sydney, School of Mathematics and Statistics, Computational Algebra Group.